RECEIVED
CENTRAL FAX CENTER
JUL 10 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Applicant: Challener	Art Unit: 2139
Serial No.: 10/748,919	Examiner: Young
Filed: December 22, 2003	RPS920030244US1
For: SYSTEM AND METHOD FOR CONTROLLING NETWORK ACCESS IN WIRELESS ENVIRONMENT	July 10, 2007 750 B STREET, Suite 3120 San Diego, CA 92101

APPEAL BRIEF

Commissioner of Patents and Trademarks

Dear Sir:

This brief is submitted under 35 U.S.C. §134 and is in accordance with 37 C.F.R. Parts 1, 5, 10, 11, and 41, effective September 13, 2004 and published at 69 Fed. Reg. 155 (August 2004). This brief is further to Appellant's Notice of Appeal filed herewith.

Table of Contents

07/12/2007 CNEGA1 00000031 503533 10748919
02 FC:1402 500.00 DA

07/13/2007 CNEGA1 00000011 503533 10748919
02 FC:1402 500.00 DA

(1) **Real Party in Interest**

The real party in interest is Lenovo (Singapore) Pte. Ltd.

(2) **Related Appeals/Interferences**

No other appeals or interferences exist which relate to the present application or appeal.

(3) **Status of Claims**

Claims 1-22 are pending and finally rejected, which rejections are appealed.

(4) **Status of Amendments**

No amendments are outstanding.

(5) **Summary of Claimed Subject Matter**

As an initial matter, it is noted that according to the Patent Office, the concise explanations under this section are for Board convenience, and do not supersede what the claims actually state, 69 Fed. Reg. 155 (August 2004), see page 49976. Accordingly, nothing in this Section should be construed as an estoppel that limits the actual claim language.

Claim 1 recites a service that includes determining that a mobile computer (reference numeral 12, figure 1; page 3, line 17) has lost connectivity to a first access point (30, figure 1; page 4, line 13) of a network (32, figure 1; page 4, line 16). When the mobile computer roams to a second access point of the network, it is determined whether the second access point is authorized for first secure communication (block

40, figure 2; page 5, second paragraph) and if so, access of the computer is released to first secure data on the network through the second access point, and otherwise access of the computer is released to data other than the first secure data on the network through the second access point, page 6, lines 4-10.

Claim 7 sets forth a mobile computer with a processor (16, figure 1; page 3, line 21 or 26, figure 1; page 4, line 8) and a wireless transceiver (24, figure 1,; page 4, line 3) in communication with the processor. The processor determines whether a predetermined communication hardware event has occurred e.g., (block 40, figure 2; page 5, second paragraph) and if so, the processor selectively configures the computer in a non-secure mode in which data on a network is accessed by the computer but not all secure data available on the network can be accessed by the computer, page 6, lines 4-10.

Claim 14 requires a system including a mobile computer (12, figure 1; page 3, line 17) and a network (32, figure 1; page 4, line 16) including secure data to includes means (e.g., 16, figure 1; page 3, line 21 executing the logic of figure 2) for determining that the mobile computer has lost connectivity to a first access point (30, figure 1; page 4, line 13) of the network, and means (e.g., 16, figure 1; page 3, line 21 or 26, figure 1; page 4, line 8 executing the logic of figure 2) for determining whether a second access point of the network to which the mobile computer has roamed is authorized for secure communication. The system also has means (e.g., hypervisor 26, figure 1; page 4, line 8 executing the logic of figure 2 as set forth at the bottom of page 5) for permitting the mobile computer to access secure data on the network through the second access point if the second access point is authorized for secure communication, and otherwise granting access to the computer to data other than the secure data through the second access point.

Claim 19 recites a method in which communication is established between a mobile computer (12, figure 1; page 3, line 17) and a network (32, figure 1; page 4, line 16) through an access point (30, figure 1;

page 4, line 13). Based on at least one of: a location, or an identification, of the access point, the method contemplates either granting the computer access to secure assets in the network or granting the computer access to other than the secure assets in the network, figure 2 and pages 4-5.

(6) Grounds of Rejection to be Reviewed on Appeal

(a) Claims 1-22, of which Claims 1, 7, 14, and 19 are independent, have been rejected under 35 U.S.C. §102 as being anticipated by Sumner et al., USPP 2003/0142641.

(b) Claims 1-22 have been rejected under 35 U.S.C. §112, second paragraph for being indefinite.

(7) Argument

a(1). Anticipation Rejections of all claims

The point of Sumner et al. is to manage roaming through various access points of a wireless local area network (WLAN) using a wireless wide area network (WWAN). At no time does Sumner et al. appear to establish the level of data access based on the access point. Appellant acknowledges that the Office Action points to paragraph 63 of Sumner et al. for the proposition that a non-secure mode is entered based on a hardware event, but all this paragraph teaches is that when connectivity is lost the computer goes to sleep to conserve power. In contrast, Claim 7, for instance requires determining whether a predetermined communication hardware event has occurred and if so selectively configuring the computer in a non-secure

mode in which data on a network is accessed by the computer but not all secure data available on the network can be accessed by the computer. The same comments apply *mutatis mutandis* to Claims 1 and 14.

Also, Sumner et al. does not use a location or identification of an access point to decide whether to grant the computer access to secure assets in the network or to grant the computer access to other than the secure assets in the network as required by Claim 19.

This has been responded to in the latest office action by resorting to paragraph 66 of Sumner et al., Office Action, top of page 9, for the proposition that Sumner teaches accessing files in a database and comparing them to local copies, and so it does. However, the examiner "interprets this to be accessing both corporate secure files and local secure files which are different." This is a puzzling argument. Nothing in the relied-upon paragraph of Sumner et al. says anything at all about secure versus non-secure files, only that the local file copy is compared against the corporate database copy. There is no discussion in any of the relied-upon portions of Sumner et al. of determining whether a second access point is authorized for communication, much less for secure communication, much less releasing access to first secure data on the network through the second access point if it is and otherwise releasing access of the computer to data other than the first secure data on the network through the second access point as required by, e.g., Claim 1.

a(2) Anticipation Rejections of Claims 3, 16, and 21

The rejections of certain dependent claims are independently reversible. Claims 3, 16, and 21 for instance require a "hypervisor", with these claims being rejected based on an alleged "definition" on page 4 of the specification. The specification, however, does not broadly define hypervisor to be anything other than what the skilled artisan would think it is, i.e., a special operating system that operates on top of the standard

O.S. The relied-upon "definition" merely observes that the hypervisor can be a dedicated part of the CPU 16 chip. Since Sumner et al. does not appear to mention "hypervisor" or any cognizable synonym, the rejections of Claims 3, 16, and 21 appear to be incorrect.

This has been responded to by bootstrapping the special purpose computer of paragraph 75 of Sumner et al. into a hypervisor. The two technologies are not coterminous nor has any evidence been adduced of record to the contrary as is otherwise required by KSR Int'l v. Teleflex, Inc., ___ S.Ct. ___ (2007) (requiring the Patent Office to produce evidence to support its findings).

a(3) Anticipation Rejections of Claims 6, 9, and 22

Apropos the rejections of Claims 6, 9, and 22 based on paragraphs 65 and 66 of Sumner et al., all these paragraphs teach in essence is roaming from point to point, not that, for any given access point with which the computer is actually communicating, access to one set of secure data is released which differs from the secure data that is released when the mobile computer is connected to another access point. This has not been responded to, conceding the point.

b. Indefiniteness Rejections of all claims

It appears that the rejection of all of claims 1-22 under this section is wrong, because the rejection appears to apply only to Claims 7-13 and 19. In any case, the Examiner has alleged that "computer" should be preceded by "mobile computer" "in all instances", but this is incorrect, see MPEP §2173.05(e) (discussion about "controlled stream of fluid"). Stated differently, the failure to repeat every modifier of a claim element

in subsequent recitations of that element does not deprive the element of proper antecedent basis under the MPEP.

Respectfully submitted,

John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1191-4.AFP

APPENDIX A - APPEALED CLAIMS

1. A service comprising:

determining that a mobile computer has lost connectivity to a first access point of a network;

when the mobile computer roams to a second access point of the network, determining whether the second access point is authorized for first secure communication and if so,

releasing access of the computer to first secure data on the network through the second access point, and otherwise releasing access of the computer to data other than the first secure data on the network through the second access point.

2. The service of Claim 1, wherein the service is undertaken by the mobile computer.

3. The service of Claim 2, wherein the service is undertaken by a hypervisor in the mobile computer.

4. The service of Claim 1, wherein the service is undertaken by at least one network resource outside the mobile computer.

5. The service of Claim 1, wherein the mobile computer is authenticated at the first access point, prior to losing connectivity thereto.

6. The service of Claim 5 wherein releasing access to secure data on the network through the second access point comprises releasing access to a set of secure data which differs from the secure data released when the mobile computer is connected to the first access point.

7. A mobile computer, comprising:

at least one processor;

at least one wireless transceiver in communication with the processor, the processor executing logic including:

determining whether a predetermined communication hardware event has occurred; and

if a predetermined communication hardware event has occurred, selectively configuring the computer in a non-secure mode in which data on a network is accessed by the computer but not all secure data available on the network can be accessed by the computer.

8. The computer of Claim 7, wherein the computer cannot access secure data on the network while configured in said non-secure mode.

9. The computer of Claim 7, wherein the computer can access a subset of the secure data on the network while configured in said non-secure mode.

10. The computer of Claim 7, wherein the predetermined hardware event is a disconnection from a wireless access point.

11. The computer of Claim 7, wherein the computer is configured in the non-secure mode if the computer roams to an access point that is not authorized for secure data transmission.

12. The computer of Claim 10, wherein the processor accesses a list of authorized access points to undertake the act of selectively configuring.

13. The computer of Claim 10, wherein the processor receives a network signal from a wireless access point to indicate whether the wireless access point is an authorized access point to undertake the act of selectively configuring.

14. A system including a mobile computer and a network including secure data, comprising:

means for determining that the mobile computer has lost connectivity to a first access point of the network;

means for determining whether a second access point of the network to which the mobile computer has roamed is authorized for secure communication; and

means for permitting the mobile computer to access secure data on the network through the second access point if the second access point is authorized for secure communication, and otherwise granting access to the computer to data other than the secure data through the second access point.

15. The system of Claim 14, wherein the means are embodied in the mobile computer.

16. The system of Claim 15, wherein the means are embodied by a hypervisor in the mobile computer.

17. The system of Claim 14, wherein the means are embodied by at least one network resource outside the mobile computer.

18. The system of Claim 14, wherein the mobile computer is authenticated at the first access point, prior to losing connectivity thereto.

19. A method comprising:

establishing communication between a mobile computer and a network through an access point; and

based on at least one of: a location, or an identification, of the access point, either granting the computer access to secure assets in the network or granting the computer access to other than the secure assets in the network.

20. The method of Claim 19, wherein the act of selectively granting is undertaken by the mobile computer.

21. The method of Claim 20, wherein the act of selectively granting is undertaken by a hypervisor in the mobile computer.

22. The method of Claim 19, wherein the computer is configured to access a first set of network assets when communicating through a first access point and a second set of network assets when communicating through a second access point.

APPENDIX B - EVIDENCE

None (this sheet made necessary by 69 Fed. Reg. 155 (August 2004), page 49978.)

APPENDIX C - RELATED PROCEEDINGS

None (this sheet made necessary by 69 Fed. Reg. 155 (August 2004), page 49978.)